MAY 2015

CYBERSECURITY BULLETIN

Borden Ladner Gervais

U.S. SECURITIES AND EXCHANGE COMMISSION ISSUES CYBERSECURITY GUIDANCE UPDATE

In April 2015, the United States Securities and Exchange Commission ("SEC") issued updated cybersecurity guidance for registered investment companies and registered investment advisers. The guidance emphasizes the importance of cybersecurity risk management, and identifies important elements of a cybersecurity risk management program.

CYBER-RISK

Cyber-risk management is an increasingly important challenge for organizations of all sizes and kinds. Cyber-risk is the risk of damage, loss and liability (e.g. financial loss, business disruption loss, loss to stakeholder value, reputational harm and legal noncompliance liability) to an organization resulting from a failure or breach of the organization's information technology systems. Cyber-risk can result from internal sources (e.g. employees, contractors, service providers and suppliers) or external sources (e.g. nation states, terrorists, hacktivists and competitors). Commentators have said that there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet.

SEC GUIDANCE

The SEC's *Guidance Update – Cybersecurity Guidance* (No. 2015-02) emphasizes the need for registered investment companies and registered investment advisers to review and improve their cybersecurity measures and related policies and practices in order to protect the security of confidential and sensitive information (including information concerning investors/clients) and to ensure compliance with legal obligations regarding identity theft and data protection, fraud and business continuity (including the ability to process shareholder transactions).

The guidance identifies three important elements of a cybersecurity risk management program:

- **Assessment:** Conduct a periodic assessment of: (1) the nature, sensitivity and location of the firm's data and relevant technology systems; (2) the internal and external cybersecurity threats to the firm and the firm's vulnerabilities; (3) the firm's current security controls and processes; (4) the potential impact of a cyber incident on the firm and other persons; and (5) the firm's governance structure for managing cybersecurity risk.
- **Strategy:** Create and periodically test a strategy to prevent, detect and respond to cybersecurity threats, including: (1) controlling access to the firm's systems and data; (2) using data encryption; (3) protecting the firm's data against loss/removal; (4) data backup; and (5) developing an incident response plan.
- **Implementation:** Implement the strategy through policies, procedures and training of the firm's personnel, monitoring compliance and educating the firm's investors/clients about managing cybersecurity risks to their accounts.

COMMENT

The SEC's guidance is a helpful summary of some basic cyber-risk management practices. Additional, more comprehensive guidance (including helpful questionnaires and checklists) is available from various regulators in the United States and Canada. Organizations of all sizes and kinds would be well served by following best practices to manage cyber-risks and prepare to respond to cyber incidents. ■

BLG Vancouver
1200 Waterfront Centre
200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744
F 604.687.1415
blg.com

Author
Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com